日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出　願　年　月　日
Date of Application:　　２００４年　４月２８日

出　願　番　号
Application Number:　　特願２００４－１３３１００

パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is　　ＪＰ２００４－１３３１００

出　願　人
Applicant(s):　　松下電器産業株式会社

２００５年　６月　８日

特許庁長官
Commissioner,
Japan Patent Office　　小　川

【書類名】　特許願
【整理番号】　2037460006
【提出日】　平成16年 4月28日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/08
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　村上　隆史
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　新谷　保之
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100097445
　【弁理士】
　【氏名又は名称】　岩橋　文雄
【選任した代理人】
　【識別番号】　100103355
　【弁理士】
　【氏名又は名称】　坂口　智康
【選任した代理人】
　【識別番号】　100109667
　【弁理士】
　【氏名又は名称】　内藤　浩樹
【手数料の表示】
　【予納台帳番号】　011305
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【包括委任状番号】　9809938

【書類名】特許請求の範囲
【請求項１】
通信媒体から受信データを受信または通信媒体へ送信データを送信する通信媒体処理手段と、
共通鍵を配信した一般通信装置のアドレスを含む一般通信装置情報と、前記一般通信装置へ配信した共通鍵の履歴を管理する配信共通鍵保持手段と、
データ送信時に最新の共通鍵、もしくはデータ送信先の一般通信装置が保持している共通鍵を前記配信共通鍵保持手段から受け取り、データを暗号化した暗号化データを通信媒体処理手段へ渡すデータ送信処理手段と、
データ受信時にデータ送信元の一般通信装置が保持している共通鍵を前記配信共通鍵保持手段から受け取り、前記共通鍵で受信データを復号化するデータ受信処理手段と、
共通鍵を生成し、システム内に前記共通鍵を配信することによって、共通鍵を更新することを要求する共通鍵更新手段とを備えたことを特徴とする共通鍵制御装置。
【請求項２】
前記共通鍵更新手段は、共通鍵の更新を設定した場合に、新しい共通鍵をランダム変数に基づき生成し、前記配信共通鍵保持手段で管理している前記一般通信装置が保持する共通鍵を更新することを特徴とする請求項１に記載の共通鍵制御装置。
【請求項３】
前記共通鍵更新手段は、前記データ送信処理手段が送信データを暗号化する際に前記配信共通鍵保持手段から受け取った共通鍵を使用する回数がある一定回数越えた場合、もしくは前記データ受信処理手段が受信データを復号化する際に前記配信共通鍵保持手段から受け取った共通鍵を使用する回数がある一定回数を越えた場合、もしくは前記データ送信処理手段が送信データを暗号化する際に前記配信共通鍵保持手段から受け取った共通鍵を使用する回数と前記データ受信処理手段が受信データを復号化する際に前記配信共通鍵保持手段から受け取った共通鍵を使用する回数との和がある一定回数越えた場合、新しい共通鍵を生成し、前記配信共通鍵保持手段で管理しているすべての前記一般通信装置が保持する共通鍵を更新することを特徴とする請求項１又は請求項２に記載の共通鍵制御装置。
【請求項４】
前記共通鍵更新手段は、前回共通鍵を更新してからある一定時間が経過した場合、新しい共通鍵を生成し、前記配信共通鍵管理保持手段で管理しているすべての前記一般通信装置が保持する共通鍵を更新することを特徴とする請求項１から請求項３のいずれか１項に記載の共通鍵制御装置。
【請求項５】
前記共通鍵更新手段は、前記データ受信処理手段が受信したデータの送信元の一般通信装置情報を前記配信共通鍵保持手段が保持しない場合、新しい共通鍵を生成し、前記配信共通鍵保持手段で管理しているすべての前記一般通信装置が保持する共通鍵を更新することを特徴とする請求項１から請求項４のいずれか１項記載の共通鍵制御装置。
【請求項６】
前記共通鍵制御装置の前記配信共通鍵保持手段は、ネットワーク上の前記一般通信装置へ配信した共通鍵の履歴を保持し、前記共通鍵ごとに配信した前記一般通信装置のアドレスを含む一般通信装置情報を管理する共通鍵管理テーブルを保持し、前記共通鍵ごとに前記一般通信装置情報を保持することによって、前記共通鍵制御装置は前記共通鍵を配信したことがある前記一般通信装置と前記共通鍵を用いて、常に暗号化したデータを送受信することが可能にすることと、前記共通鍵を管理するための前記共通鍵管理テーブルのリソースを削減することを特徴とする請求項１から請求項４のいずれか１項に記載の共通鍵制御装置。
【請求項７】
共通鍵を配信する際、前記共通鍵を暗号化するための初期共通鍵を特定の手段を用いて入力する機能を持つ初期共通鍵入力手段を保持することを特徴とする請求項１から請求項６のいずれか１項に記載の共通鍵制御装置。

【請求項８】
前記初期共通鍵入力手段は、キーボード、タッチパネル、マウスといった入力装置を使用して前記初期共通鍵を入力することを特徴とする請求項７に記載の共通鍵制御装置。
【請求項９】
前記初期共通鍵入力手段は、前記共通鍵の配信先である一般通信装置のリモコンの信号を受け取る受光部であり、リモコンを使用して前記初期共通鍵を入力することを特徴とする請求項７に記載の共通鍵制御装置。
【請求項１０】
前記初期共通鍵入力手段は、一般通信装置本体へ記されていたり、一般通信装置を梱包する袋や箱に記されていたりする符号を読み取る装置であり、前記一般通信装置の符号を読み取ることで前記初期共通鍵を入力することを特徴とする請求項７に記載の共通鍵制御装置。
【請求項１１】
前記初期共通鍵入力手段は、記憶媒体をインストールすることができる装置であり、前記記憶媒体をインストールすることによって前記初期共通鍵を入力することを特徴とする請求項７に記載の共通鍵制御装置。
【請求項１２】
通信媒体からデータを受信又は通信媒体へデータを送信する通信媒体処理手段と、
共通鍵制御装置から配信された共通鍵と、前記共通鍵制御装置が管理するすべての前記一般通信装置が保持する共通鍵を更新している時の配信状態を示す共通鍵配信状態とを保持する共通鍵保持手段と、
データ送信時に前記共通鍵保持手段から前記共通鍵配信状態に適した共通鍵を受け取り、データを暗号化した暗号化データを通信媒体処理手段へ渡すデータ送信処理手段と、
データ受信時に前記共通鍵保持手段から前記共通鍵配信状態に適した共通鍵を受け取り、前記共通鍵で受信データを復号化するデータ受信処理手段と、
前記共通鍵制御装置へ最新の共通鍵の配信要求用データを作成し、前記データ送信処理手段へ渡す共通鍵要求手段とを備えたことを特徴とする一般通信装置。
【請求項１３】
前記共通鍵要求手段は、最新の共通鍵の更新漏れを回避するために、通信できない状態であった前記一般通信装置がシステム内へ再参入する際、最新共通鍵の配信要求用のデータを作成することを特徴とする請求項１２に記載の一般通信装置。
【請求項１４】
前記一般通信装置の前記共通鍵保持手段が保持する前記共通鍵配信状態は、前記一般通信装置は共通鍵を配信されていないことを示す未設定状態、または、前記一般通信装置が前記共通鍵制御装置から共通鍵の更新要求を受信したことを示す配信完了状態、または、共通鍵を前記一般通信装置へ更新中であることを示す移行中状態、または、すべての一般通信装置が共通鍵の更新を完了したことを示す更新完了状態といった状態を保持することを特徴とする請求項１２または請求項１３に記載の一般通信装置。
【請求項１５】
前記一般通信装置の共通鍵保持手段が保持する前記共通鍵配信状態が配信完了状態である場合、前記一般通信装置は送信データを暗号化する場合、前記前共通鍵を使用して前記送信データを暗号化して送信することを特徴とする請求項１２から請求項１４のいずれか１項に記載の一般通信装置。
【請求項１６】
前記一般通信装置の共通鍵保持手段が保持する前記共通鍵配信状態が配信完了状態である場合、前記一般通信装置は受信データを復号化する場合、前記前共通鍵と前記新共通鍵とを使用して前記受信データを復号化し、前記前共通鍵と前記新共通鍵のどちらの共通鍵で前記受信データを暗号化されたかを特定し、前記受信データで指定する処理を行うことを特徴とする請求項１２から請求項１４のいずれか１項に記載の一般通信装置。
【請求項１７】

前記一般通信装置の共通鍵保持手段が保持する前記共通鍵配信状態が移行中状態である場合、前記一般通信装置は送信データを暗号化する場合、前記新共通鍵を使用して前記送信データを暗号化して送信することを特徴とする請求項１２から請求項１４のいずれか１項に記載の一般通信装置。

【請求項１８】

前記一般通信装置の共通鍵保持手段が保持する前記共通鍵配信状態が移行中状態である場合、前記一般通信装置は受信データを復号化する場合、前記前共通鍵と前記新共通鍵とを使用して前記受信データを復号化し、前記前共通鍵と前記新共通鍵のどちらの共通鍵で前記受信データを暗号化されたかを特定し、前記受信データで指定する処理を行うことを特徴とする請求項１２から請求項１４のいずれか１項に記載の一般通信装置。

【請求項１９】

前記一般通信装置の共通鍵保持手段が保持する前記共通鍵配信状態が更新完了状態である場合、前記一般通信装置は送信データを暗号化する場合、前記新共通鍵を使用して前記送信データを暗号化して送信することを特徴とする請求項１２から請求項１４のいずれか１項に記載の一般通信装置。

【請求項２０】

前記一般通信装置の共通鍵保持手段が保持する前記共通鍵配信状態が更新完了状態である場合、前記一般通信装置は受信データを復号化する場合、前記新共通鍵を使用して前記受信データを復号化し、前記受信データで指定する処理を行うことを特徴とする請求項１２から請求項１４のいずれか１項に記載の一般通信装置。

【書類名】明細書
【発明の名称】共通鍵制御装置および一般通信装置
【技術分野】
【０００１】
ネットワークへ接続する機器へ新規に共通鍵を更新する場合、すでに配信している共通鍵を用いて、１台ずつ新規の共通鍵を暗号化して更新する場合、時間差が生じ、新規の共通鍵を保持している機器と保持していない機器がネットワーク内に存在することになる。そのような場合においても、常にネットワークに接続している機器同士で通信可能とするように制御する通信制御装置に関するものである。
【背景技術】
【０００２】
従来の通信制御装置では、共通鍵を管理する通信制御装置は共通鍵を配信するだけで、その他のすべてのネットワークに接続している機器がネットワーク上に配信した共通鍵の履歴を保持するものとしていた（例えば、特許文献１参照）。すべての機器が配信された共通鍵を保持している。例えば、送信元の機器は送信データを暗号化した共通鍵を特定するために送信データの非暗号化部に共通鍵番号を付与して、送信先の機器へデータを送信する。そして、データを受信した送信先の機器は、受信データに付与している共通鍵番号から受信データを復号化するための共通鍵を選択し、受信データを復号する。このような方法によって、送信元でデータを暗号化する共通鍵と送信先でデータを復号化する共通鍵を同じものを使用した通信を実現することが可能としていた。
【特許文献１】特開２００３－１０１５３３号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかしながら、前記従来の構成では、共通鍵の履歴をすべての機器が保持する必要があり、リソースの小さい白物家電、センサ類といったネットワークに接続する機器では配信されたすべての共通鍵の履歴を保持することは難しいという課題を有していた。
【０００４】
さらに、リソースが小さく、共通鍵の履歴管理を行うことができないという理由で、配信された共通鍵を一つしか持たないような機器でネットワークを構成した場合、新たな課題が発生する。新たな課題とは、ネットワークに接続する機器が複数存在している場合、すべての機器に対して共通鍵を更新すると、共通鍵を更新する順番によって、更新後の共通鍵を保持している機器と更新前の共通鍵を保持する機器が同時に存在する場合が発生する。その時、共通鍵を更新済みの機器と、共通鍵を未更新の機器とで暗号化したデータを用いて通信を行うことができない。
【課題を解決するための手段】
【０００５】
前記、従来の課題を解決するために、本発明の通信制御装置では、共通鍵を配信する装置は共通鍵更新状態管理手段と配信共通鍵保持手段を有して、共通鍵を配信される機器の負担を軽減するために共通鍵の管理を行う。
【０００６】
負担を軽減化された共通鍵を配信される機器側は、共通鍵の更新状態を保持し、その状態によって保持する共通鍵の種類、データの暗号化、復号化に使用する共通鍵の選択を行う。ただし、保持する共通鍵は最大でも更新後の共通鍵および更新前の共通鍵の二種類を保持する。従来の課題を解決するために、更新後の共通鍵と更新前の共通鍵を共通鍵の更新状態によって使い分ける。従って、更新後の共通鍵を保持する機器と更新前の共通鍵を保持する機器間の通信においても、データを暗号化して通信を行うことを可能とする。
【発明の効果】
【０００７】
特にホームネットワークを考慮した場合、通信システムは１：１や１：Ｎではなく、Ｍ

・Nによって構成される。M・Nの通信システムである場合、共通鍵を配信される機器間士の通信が行われる。共通鍵を更新している間では、更新後の共通鍵を保持する機器と更新前の共通鍵を保持する機器の間で通信が発生する可能性があるが、そのような場合においても、データを暗号化して通信を行うことができる。つまり、リソースが小さく共通鍵を配信される機器は、共通鍵の配信履歴を保持する必要なく、システム内の最新の共通鍵を保持する機器と保持していない機器間において通信することを可能とする。

【発明を実施するための最良の形態】

【０００８】

以下本発明の実施の形態について、図面を参照しながら説明する。

【０００９】

（実施の形態１）

図１は、本発明の実施の形態１における有線もしくは無線である通信媒体１３に、共通鍵制御装置１１と複数の一般通信装置１２が接続しているシステム構成図である。共通鍵制御装置１１は、通信媒体１３に接続している一般通信装置１２へ共通鍵を配信するとともに、一般通信装置１２ごとに配信している共通鍵や、共通鍵の一般通信装置１２への共通鍵配信状態や、配信した共通鍵の履歴を管理している。共通鍵とは、通信システム内の一般通信装置１２及び共通鍵制御装置１１が処理するデータを暗号・復号化する際に用いる同一の鍵である。共通鍵の一般通信装置１２への共通鍵配信状態には、共通鍵を配信していない「未設定状態」、共通鍵の更新を受信した直後の状態を「配信完了状態」、システム全体で更新後の共通鍵を保持している一般通信装置１２と、更新前の共通鍵を保持している一般通信装置１２が混在している「移行中状態」、システム全体ですべての一般通信装置１２が更新後の共通鍵を保持している「更新完了状態」といった状態がある。共通鍵配信状態の詳細な説明は後述する。

【００１０】

図２は、有線もしくは無線である通信媒体２２に接続する共通鍵制御装置１１のプロトコルスタックを示した図である。通信媒体処理手段２３は、通信媒体２２へ送信データを送信し、受信データを通信媒体２２から受信する。データ受信処理手段２４は、通信媒体処理手段２３から受信データを受け取ると、後述する配信共通鍵保持手段２６から受信データの送信元へ配信している共通鍵を受け取り、受信データを復号化する。データ送信処理手段２５は、後述する配信共通鍵保持手段２６から送信データの送信先へ配信している共通鍵を受け取り、送信データを暗号化して通信媒体処理手段２３へ渡す。ただし、送信先を特定しない例えばブロードキャストやマルチキャストでデータを送信する場合、後述する配信共通鍵保持手段２６からシステム全体での最新の共通鍵を受け取り、送信データを暗号化して通信媒体処理手段２３へ渡す。

【００１１】

配信共通鍵保持手段２６は、図５で示すような共通鍵を管理するためのテーブル５１を保持している。このテーブル５１の特長については、後述する。配信共通鍵保持手段２６は更新した共通鍵の履歴を管理するとともに、一般通信装置１２ごとに配信した共通鍵を保持しており、データ受信処理手段２４がデータを受信する際、送信元の一般通信装置１２が保持している共通鍵をデータ受信処理手段２４へ渡し、データ送信処理手段２５がデータを送信する際、送信先の一般通信装置１２が保持している共通鍵をデータ送信処理手段２５へ渡す。また、配信共通鍵保持手段２６は、一般通信装置１２から共通鍵の更新を要求するデータを受信すると、送信元の一般通信装置１２へ最新の共通鍵を配信する。共通鍵更新手段２７は、共通鍵を更新する際、新しい共通鍵を生成し、一般通信装置１２へ配信する。

【００１２】

新しい共通鍵を生成する方法として、例えばランダムで変数を作成することによって、共通鍵を生成するといった方法がある。共通鍵を更新するタイミングとしては、例えば以下のタイミングが存在する。システム使用者が、共通鍵制御装置の画面や本体から手動で更新を指定するタイミングで共通鍵を更新する。また、最新の共通鍵を使用して送信デー

ノを暗号化及び受信データを復号した回数がある一定回数に達したタイミングで、共通鍵を更新する。また、定期的に共通鍵を配信してから一定の時間が経過したタイミングで、共通鍵を更新する。また、配信共通鍵保持手段２６で管理していない一般通信装置１２から、管理している一般通信装置１２へ配信した共通鍵を使用して暗号化されたデータを受信したタイミングで、共通鍵を更新する。

【００１３】

図３は、有線もしくは無線である通信媒体３２に接続する一般通信装置１２のプロトコルスタックを示した図である。通信媒体処理手段３３は、通信媒体３２へ送信データを送信し、受信データを通信媒体３２から受信する。データ受信処理手段３４は、通信媒体処理手段３３から受信データを受け取ると、後述する共通鍵保持手段３６から自己の共通鍵配信状態に適した共通鍵を受け取り、受信データを復号化する。データ送信処理手段３５は、後述する共通鍵保持手段３６から自己の共通鍵配信状態に適した共通鍵を受け取り、送信データを暗号化して通信媒体処理手段３３へ渡す。共通鍵保持手段３６は、自己の共通鍵配信状態と共通鍵を保持し、共通鍵配信状態に適した共通鍵をデータ受信処理手段３４及びデータ送信処理手段３５へ渡す。電源ＯＦＦの状態などネットワークから離脱していた一般通信装置１２がネットワークへ参入した際に、共通鍵の更新漏れを回避するために、共通鍵要求手段３７は共通鍵制御装置１１へ最新の共通鍵を配信することを要求する。

【００１４】

図１に示すシステムのように、複数の一般通信装置１２がシステム内に存在する場合、共通鍵制御装置１１が共通鍵を更新する場合、システム内には更新前の共通鍵を保持する一般通信装置１２と、更新後の共通鍵を保持する一般通信装置１２が存在する。更新後の共通鍵を保持する一般通信装置１２と保持していない一般通信装置１２間の通信を可能とするための共通鍵更新シーケンスを図４に示す。

【００１５】

更新前の共通鍵を「前共通鍵」、更新後の共通鍵を「新共通鍵」と呼ぶこととする。共通鍵制御装置１１が管理している各一般通信装置１２は、前共通鍵を保持しており、共通鍵配信状態は更新完了状態である。このとき、一般通信装置１２はデータを送信する場合のデータの暗号化及びデータを受信した場合のデータの復号化には、前共通鍵を使用する。共通鍵制御装置１１は、自己が管理しているすべての一般通信装置１２に対して、前共通鍵で新共通鍵を暗号化して新共通鍵を配信する。新共通鍵を受信した一般通信装置１２は、共通鍵配信状態を配信完了状態へ遷移させる。共通鍵配信状態が配信完了状態であるとき、一般通信装置１２はデータを送信する場合のデータの暗号化には前共通鍵を使用し、データを受信した場合のデータの復号化には新共通鍵もしくは前共通鍵を使用し、新共通鍵もしくは前共通鍵のどちらで暗号化されたデータであるかを確認する。

【００１６】

共通鍵制御装置１１は、管理するすべての一般通信装置１２へ新共通鍵を配信するデータを送信した後で、管理するすべての一般通信装置１２の共通鍵配信状態を移行中状態に設定するためのデータを送信する。共通鍵配信状態が移行中状態であるとき、一般通信装置１２はデータを送信する場合のデータの暗号化には新共通鍵を使用し、データを受信した場合のデータの復号化には新共通鍵もしくは前共通鍵を使用し、新共通鍵もしくは前共通鍵のどちらで暗号化されたデータであるかを確認する。そして、共通鍵制御装置１１は、管理するすべての一般通信装置１２へ新共通鍵を配信し、すべての一般通信装置の共通鍵配信状態を移行中状態に設定できたことを確認した場合、通信管理装置１１は、すべての一般通信装置１２の共通鍵配信状態を更新完了状態に設定する。更新完了状態を設定された一般通信装置１２は、データを送信する場合のデータの暗号化及びデータを受信した場合のデータの復号化には、前共通鍵を使用する。

【００１７】

また、特に一般通信装置が家電機器やセンサ類である場合、共通鍵更新時にネットワークに接続していない可能性がある。その場合、共通鍵制御装置１１は、一般通信装置１２

の共通鍵配信状態を更新完了状態には設定しない。共通鍵配信状態を用いながら更新シーケンスを実行することによって、共通鍵更新中に新共通鍵に更新された一般通信装置１２と新共通鍵に更新されていない一般通信装置１２がシステム内に混在している場合においても、一般通信装置１２同士で共通鍵を使用した通信を可能とすることができる。また、一般通信装置１２は、共通鍵配信状態が配信完了状態、移行中状態のときのみ新共通鍵と前共通鍵を保持し、更新完了状態の場合は新共通鍵を保持するだけでよく、一般通信装置１２がリソースの小さい家電機器やセンサ類であるとしても、対応が可能である。

【００１８】

図５に、共通鍵制御装置１１の配信共通鍵保持手段２６で保持する共通鍵管理テーブル５１を示す。配信共通鍵保持手段２６で保持する共通鍵を配信した機器ごとに管理するテーブルの特長を記載する。図５に示すように、共通鍵管理テーブルでは共通鍵を配信した履歴を管理しており、共通鍵を配信した一般通信装置１２のネットワーク上のアドレスを合わせて記している。図５では、最新共通鍵はアドレスＡ、アドレスＢ、アドレスＣの一般通信装置へ配信することができており、アドレスＤの一般通信装置は最新の共通鍵の更新ができておらず一つ前の共通鍵である共通鍵履歴１を保持している。アドレスＥ、アドレスＦの一般通信装置は、共通鍵履歴１及び最新共通鍵への更新ができておらず共通鍵履歴２を保持している。共通鍵履歴３を保持する一般通信装置はシステム内には存在しておらず、アドレスＧの一般通信装置は共通鍵履歴３以降の共通鍵の更新ができておらず共通鍵履歴４を保持している。このように、共通鍵制御装置１１は配信した共通鍵ごとに配信先の一般通信装置のアドレスを管理することによって、常に一般通信装置１２が保持する共通鍵を使用して、一般通信装置１２へデータを暗号化して送信することができ、また、一般通信装置１２から受信したデータを復号化することが可能となる。

【００１９】

また、配信した共通鍵を管理する際、共通鍵管理テーブル５１のように、配信した共通鍵の履歴ごとに配信先の一般通信装置のアドレスを管理する。また、配信していない共通鍵の履歴は削除することができる。そうすることによって、不揮発性のメモリに登録する場合でも、揮発性のメモリに登録する場合でも、共通鍵の履歴を管理する上で、最低限のメモリ使用量で、各一般通信装置へ配信した共通鍵を管理することが可能である。

【００２０】

図６は、図２で示した共通鍵制御装置１１のプロトコルスタックに初期共通鍵入力手段６８を追加した図である。初期共通鍵入力手段６８は、配信共通鍵保持手段２６にて管理していない一般通信装置宛てへ共通鍵を配信する際、共通鍵を暗号化するための初期共通鍵を入力する手段である。初期共通鍵は、配信先の一般通信装置が保持する共通鍵である。

【００２１】

一般通信装置に配信している共通鍵を外部の第三者から共通鍵を盗まれずに更新するために、前述したように、前共通鍵で新共通鍵を暗号化して新共通鍵を送信する。しかし、共通鍵を配信したことがない一般通信装置へ、共通鍵を配信する場合、共通鍵を暗号化するための前共通鍵が配信共通鍵保持手段にて保持していない。従って、初期共通鍵入力手段６８から共通鍵を配信する一般通信装置１２が保持する初期共通鍵を入力する必要がある。

【００２２】

初期共通鍵入力手段６８は、例えばキーボードやタッチパネルを使用して、一般通信装置が保持する初期共通鍵を手動で入力するものである。

【００２３】

また、初期共通鍵入力手段６８は、例えば一般通信装置が家電機器などである場合、その該当する家電機器のリモコンから信号を受信できる受光部であり、リモコンを使用して一般通信装置が保持する初期共通鍵を入力するものである。

【００２４】

また、初期共通鍵入力手段６８は、例えばバーコードリーダーであり、その該当する一

般通信装置のバーコードを読み取ることにより、一般通信装置が保持する初期共通鍵を入力するものである。

【００２５】

また、初期共通鍵入力手段６８は、例えばＳＤカード、フロッピー（登録商標）ディスク、ＣＤ－Ｒなどの通信一般装置に添付している記憶媒体を読み取ることができる装置であり、インストールされた記憶媒体から一般通信装置が保持する初期共通鍵を読出して入力するものである。

【００２６】

また、図７に家の外にセンタサーバ７１が存在しているシステムについて記載する。センタサーバ７１は通信制御装置６１や一般通信装置１２といった機器の初期共通鍵を含むその機器に関するすべての情報を保持している。まず、初期共通鍵入力手段６８は、共通鍵の配信先の一般通信装置１２からその一般通信装置１２の情報、例えばメーカコード、商品コード、製造番号、製造年月日を取得する。それらの情報の組合せ、もしくは単体の情報を家７２の外にあるセンタサーバ７１へインターネットを経由して渡し、その情報をもとにセンタサーバ７１から該当する一般通信装置１２が保持する初期共通鍵を取得して入力するものである。ただし、初期共通鍵を取得するためのセンタサーバ７１と家７２の間のインターネットを利用した通信網は、第三者が通信内容を傍受しても判断できないように、暗号化されていることが必要である。

【００２７】

実際のホームネットワークにおける具体例を記載する。ホームネットワークの構成を図８に示す。図８に示すように、共通鍵制御装置であるコントローラ８１と一般通信装置であるエアコン８２、センサ８３でホームネットワークを構成するものとする。例えば、センサは検知状態ありに変化した場合、エアコンへ動作開始の制御を行い、センサは検知状態なしに変化した場合、エアコンへ動作停止の制御を行うこととする。

【００２８】

最初に、共通鍵制御装置であるコントローラ８１が一般通信装置であるエアコン８２、センサ８３の順に共通鍵を更新する場合について記載する。コントローラ８１が共通鍵更新のシーケンスを実行中、つまり、エアコン８２の共通鍵を更新したが、センサ８３の共通鍵をまだ更新していないときに、センサ８３が検知状態ありに状態が変化し、更新前の共通鍵でデータを暗号化して、エアコン動作開始の制御要求を送信する。このとき、エアコン８２の共通鍵配信状態は「配信完了」である。従って、エアコン８２は受信したデータを更新後の共通鍵で復号し、暗号化した共通鍵と異なっていることを判断すると、更新前の共通鍵で受信データを復号化する。この結果、エアコン８２はセンサ８３から動作開始要求データを受付けることができる。この例は、送信先のエアコン８２と送信元のセンサ８３の保持する共通鍵が異なる場合である。その後、コントローラ８１はセンサ８３に共通鍵を配信し、センサ８３は共通鍵配信状態を内部的に「配信完了」に遷移させる。次に、コントローラ８１は、共通鍵配信状態を「移行中」へ移行するようにエアコン８２、センサ８３の順番に要求する。エアコン８２に共通鍵配信状態を「移行中」へ移行する要求データを送信後に、センサ８３の検知状態が「なし」へ変化した。このとき、センサ８３の共通鍵配信状態は「配信完了」であるため、更新前の共通鍵を使用してエアコン８２動作停止要求データを暗号化して送信する。

【００２９】

受信したエアコン８３は、共通鍵配信状態が「移行中」であるため、受信したデータを更新後の共通鍵で復号し、暗号化した共通鍵と異なっていることを判断すると、更新前の共通鍵で受信データを復号化する。この結果、エアコン８２はセンサ８３から動作停止要求データを受付けることができる。その後、コントローラ８１はセンサ８３に共通鍵配信状態を「移行中」に移行するように要求データを送信する。次に、コントローラ８１は、共通鍵配信状態を「更新完了」へ移行するようにエアコン８２、センサ８３の順番に要求する。エアコン８２に共通鍵配信状態を「更新完了」へ移行する要求データを送信後に、センサ８３の検知状態が「あり」へ変化した。このとき、センサ８３の共通鍵配信状態は

「移行中」であるため、更新後の共通鍵を使用してエアコン動作開始要求データを暗号化して送信する。受信したエアコン８３は、共通鍵配信状態が「更新完了」であるため、受信したデータを更新後の共通鍵で復号する。この結果、エアコン８２はセンサ８３から動作開始要求データを受付けることができる。

【００３０】

次に、コントローラ８１がセンサ８３、エアコン８２の順に共通鍵を更新する場合について記載する。コントローラ８１が共通鍵更新のシーケンスを実行中、つまり、センサ８３の共通鍵を更新したが、エアコン８２の共通鍵をまだ更新していないときに、センサ８３が検知状態ありに状態が変化し、エアコン８２動作開始の制御要求データを暗号化して送信する。このとき、センサ８３の共通鍵配信状態は「配信完了」である。従って、センサ８３は、更新後の共通鍵を保持しているが、更新前の共通鍵を使用してエアコン８２動作開始の制御要求データを暗号化して送信する。

【００３１】

エアコン８２は受信したデータを、保持している更新前の共通鍵で受信データを復号化する。この結果、エアコン８２はセンサ８３から動作開始要求データを受付けることができる。この例は、送信先のエアコン８２と送信元のセンサ８３の保持する共通鍵が異なる場合である。その後、コントローラ８１はエアコン８２に共通鍵を配信し、エアコン８２は共通鍵配信状態を内部的に「配信完了」へ遷移させる。

【００３２】

次に、コントローラ８１は、共通鍵配信状態を「移行中」へ移行するようにセンサ８３、エアコン８２の順番に要求する。センサ８３に共通鍵配信状態を「移行中」へ移行する要求データを送信後に、センサ８３の検知状態が「なし」へ変化した。このとき、センサ８３の共通鍵配信状態は「移行中」であるため、更新後の共通鍵を使用してエアコン８２動作停止要求データを暗号化して送信する。受信したエアコン８３は、共通鍵配信状態が「配信完了」であるため、受信したデータをまず更新後の共通鍵で受信データを復号し、暗号化した共通鍵と同一であることを確認する。その場合、更新前の共通鍵で受信データを復号化する必要はない。この結果、エアコン８２はセンサ８３から動作停止要求データを受付けることができる。その後、コントローラ８１はエアコン８２に共通鍵配信状態を「移行中」に移行するように要求データを送信する。

【００３３】

次に、コントローラ８１は、共通鍵配信状態を「更新完了」へ移行するようにセンサ８３、エアコン８２の順番に要求する。センサ８３に共通鍵配信状態を「更新完了」へ移行する要求データを送信後に、センサ８３の検知状態が「あり」へ変化した。このとき、センサ８３の共通鍵配信状態は「更新完了」であるため、更新後の共通鍵を使用してエアコン動作開始要求データを暗号化して送信する。

【００３４】

受信したエアコン８３は、共通鍵配信状態が「移行中」であるため、受信したデータをまず更新後の共通鍵で受信データを復号し、暗号化した共通鍵と同一であることを確認する。その場合、更新前の共通鍵で受信データを復号化する必要はない。この結果、エアコン８２はセンサ８３から動作開始要求データを受付けることができる。

【００３５】

このような現象は、ホームネットワークのようにＭ：Ｎの通信システムにおいて、発生する可能性は十分高い。また、低速の通信媒体を使用している場合においては、共通鍵の更新には、さらに時間も要することとなるが、その場合も常に一般通信装置間において、通信を行うことが可能である。

【００３６】

尚、本発明はプログラムによって実現することも可能である。

【産業上の利用可能性】

【００３７】

本発明にかかる通信制御装置は、特にホームネットワークのようにＭ：Ｎの通信を行う

システムに使用すると、共通鍵を更新している間に、システム内で更新された共通鍵を保持する機器と、保持しない機器との間でも通信を行うことが可能となる。また、本発明にかかる通信制御装置を使用して共通鍵を管理することによって、特にリソースの小さい家電機器などの一般通信装置に組込むことによって効果は大きくなる。

【図面の簡単な説明】

【００３８】

【図１】システム構成図

【図２】共通鍵制御装置のプロトコルスタック図

【図３】一般通信装置のプロトコルスタック図

【図４】共通鍵更新時のシーケンス図

【図５】共通鍵管理テーブルの一例を示す図

【図６】共通鍵制御装置のプロトコルスタック図

【図７】センタサーバが存在する場合のシステム構成図

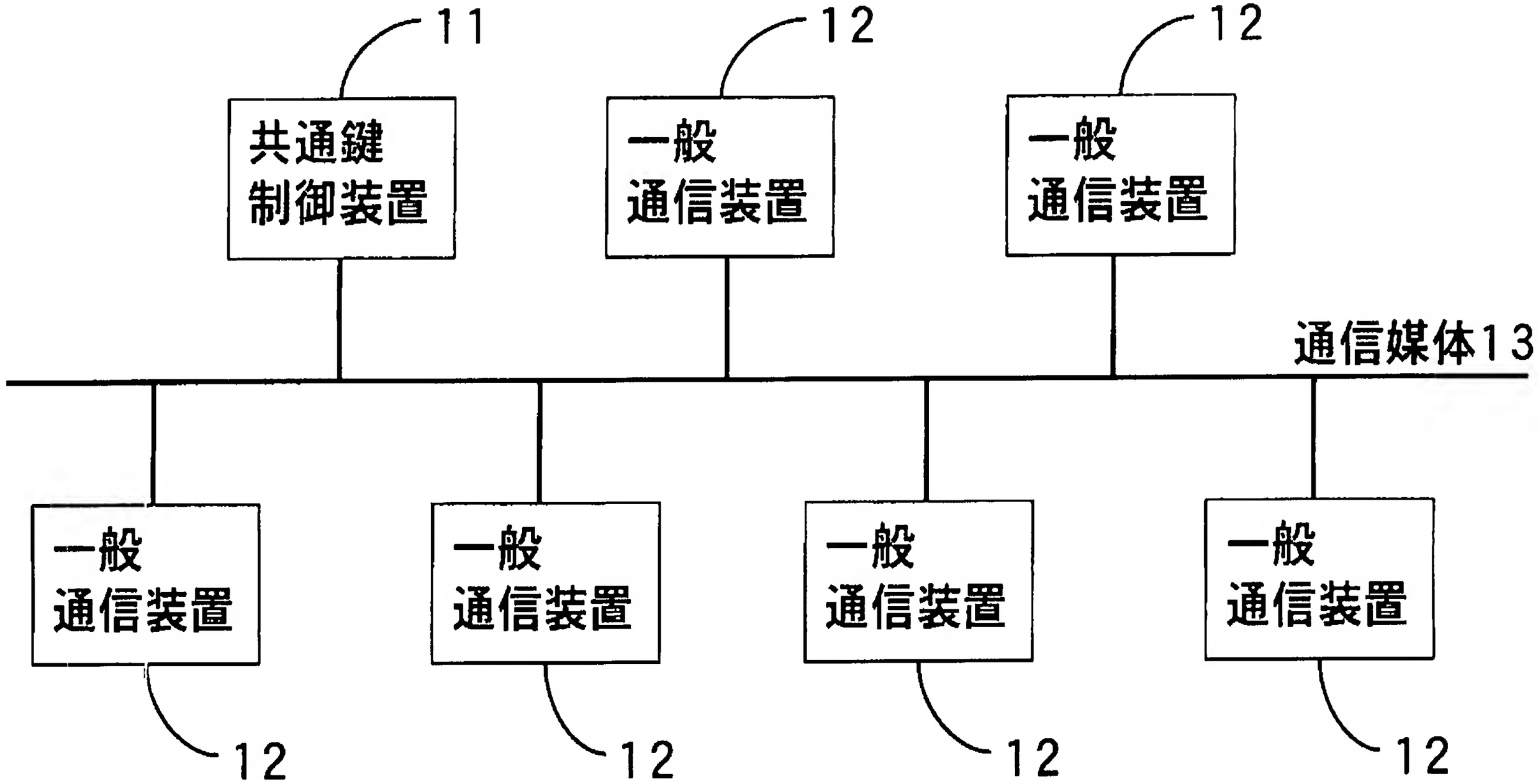
【図８】ホームネットワークのシステム構成図

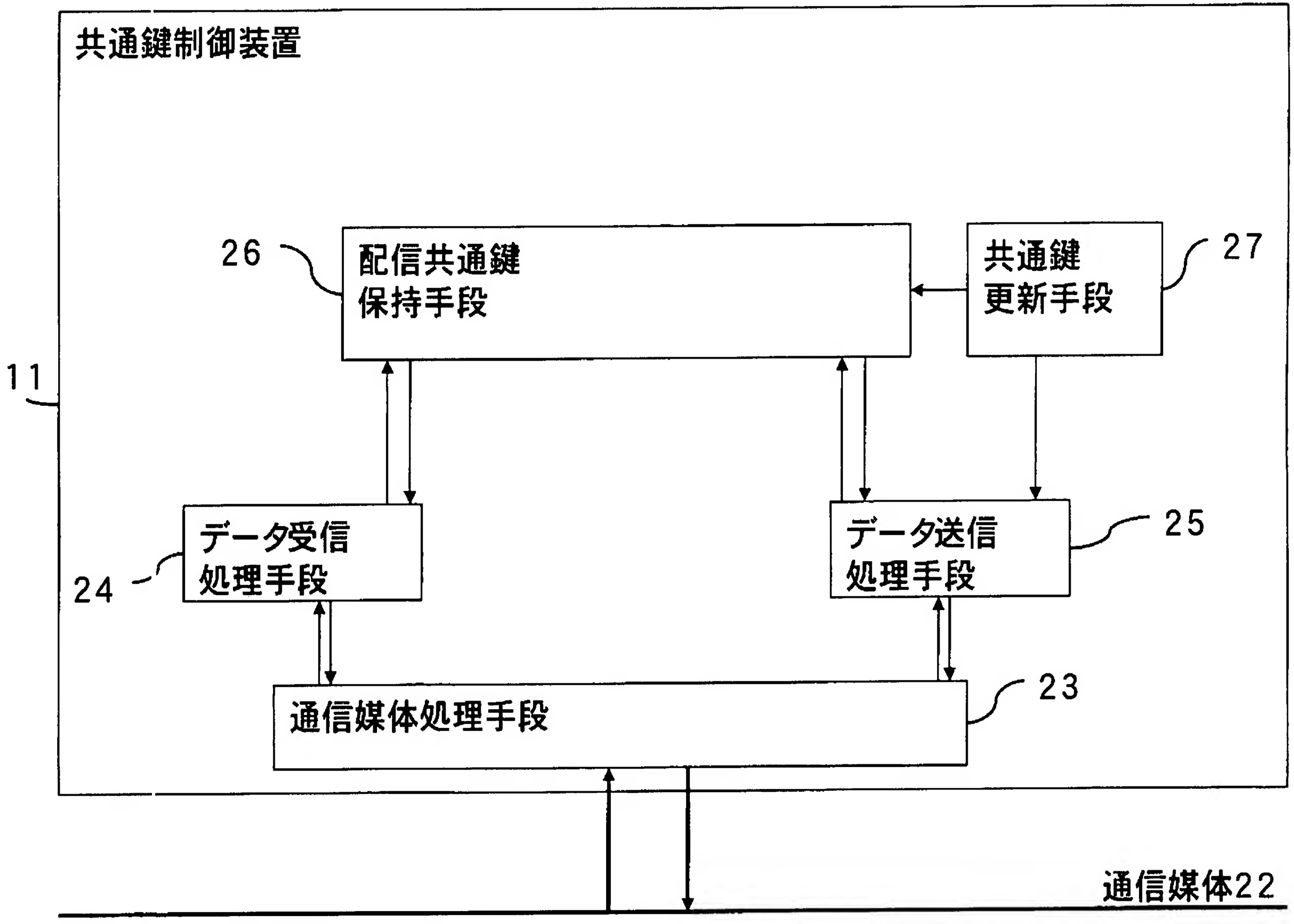
【符号の説明】

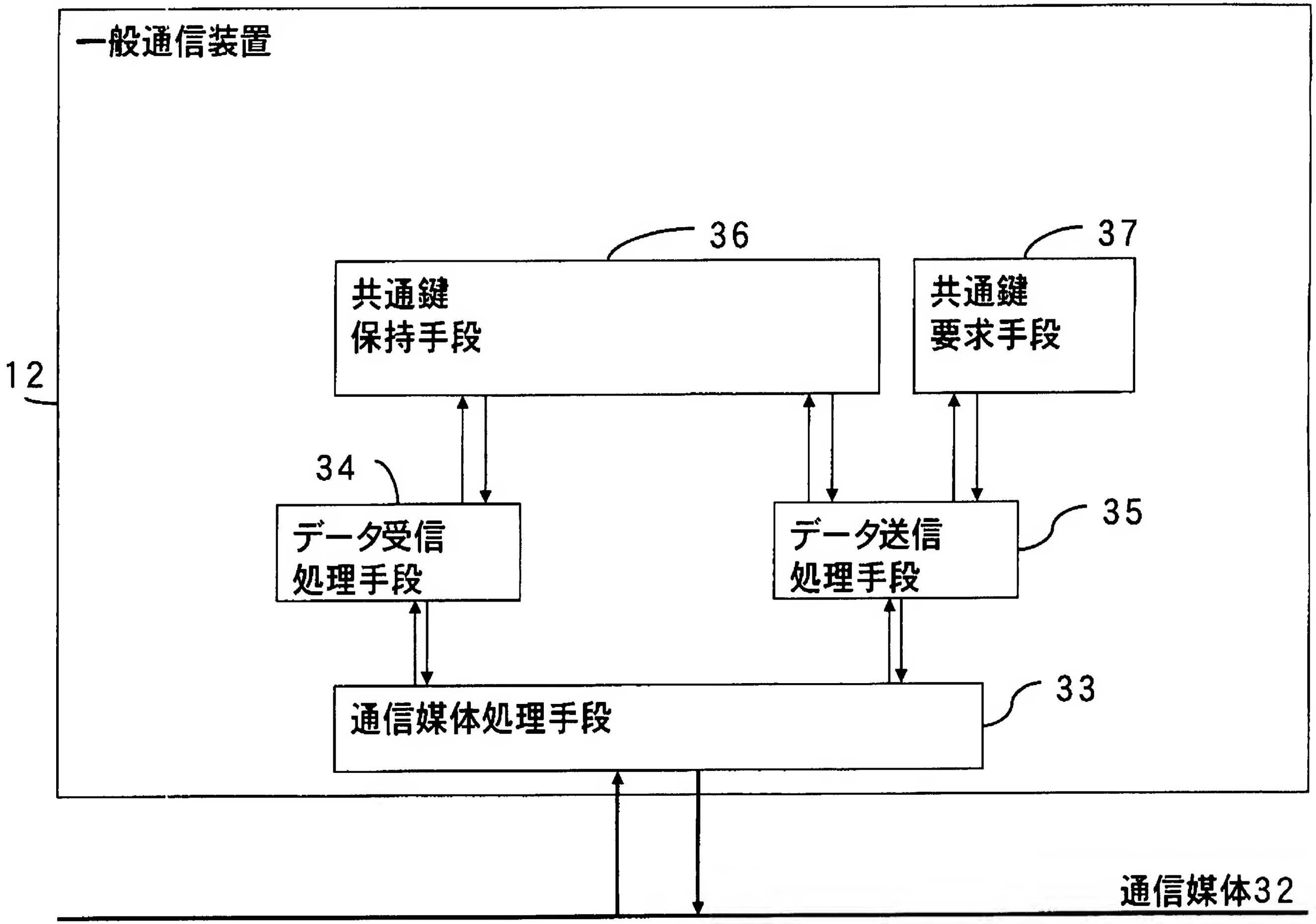
【００３９】

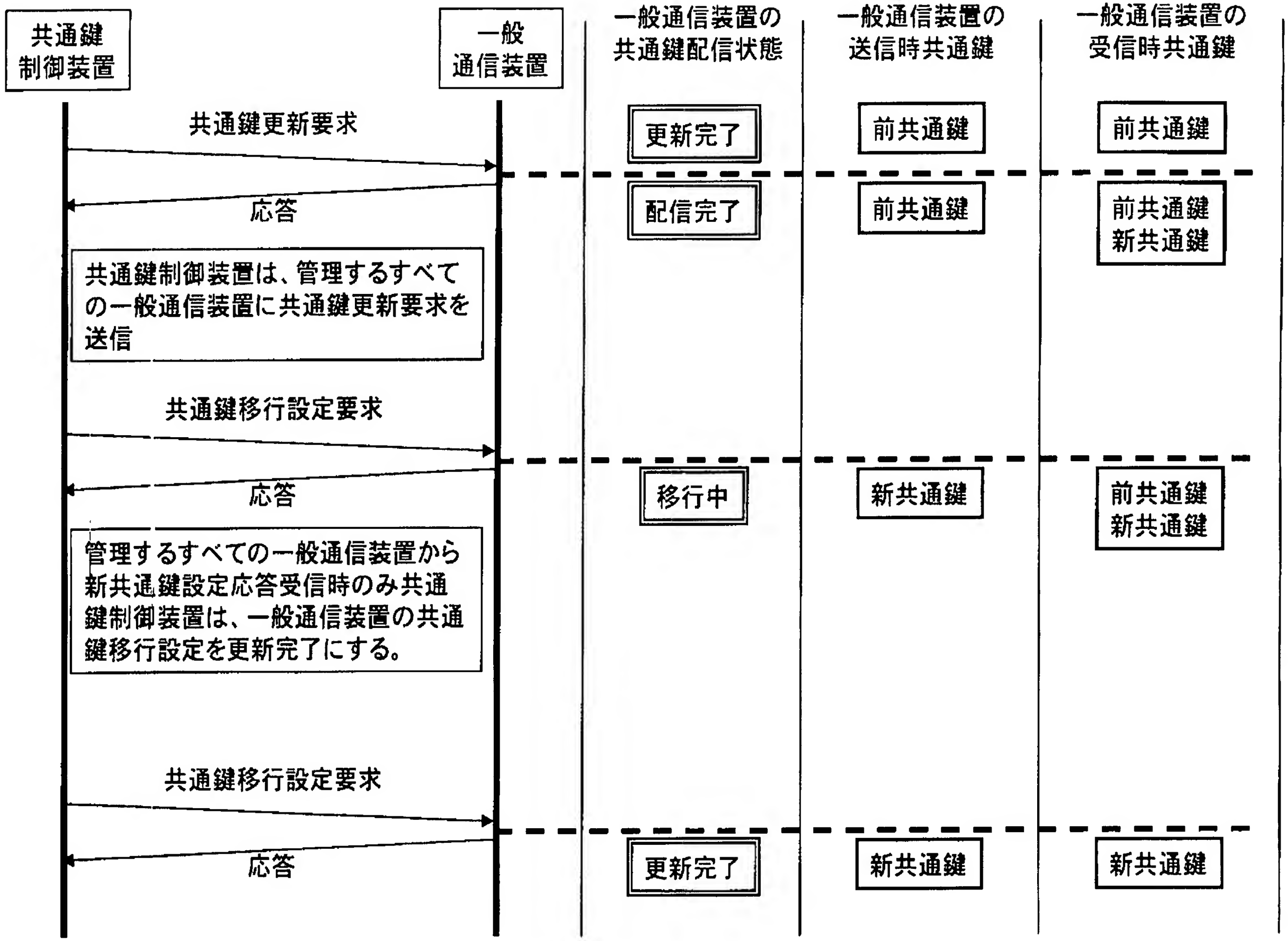
１１　共通鍵制御装置
１２　一般通信装置
１３　通信媒体
２２　通信媒体
２３　通信媒体処理手段
２４　データ受信処理手段
２５　データ送信処理手段
２６　配信共通鍵保持手段
２７　共通鍵更新手段
３２　通信媒体
３３　通信媒体処理手段
３４　データ受信処理手段
３５　データ送信処理手段
３６　共通鍵保持手段
３７　共通鍵要求手段
５１　共通鍵管理テーブル
６１　共通鍵制御装置
６８　初期共通鍵入力手段
７１　センタサーバ
７２　家
８１　コントローラ（共通鍵制御装置）
８２　エアコン（一般通信装置）
８３　センサ（一般通信装置）

【図１】


11
12
12
共通鍵
制御装置
一般
通信装置
一般
通信装置
通信媒体13
一般
通信装置
一般
通信装置
一般
通信装置
一般
通信装置
12
12
12
12

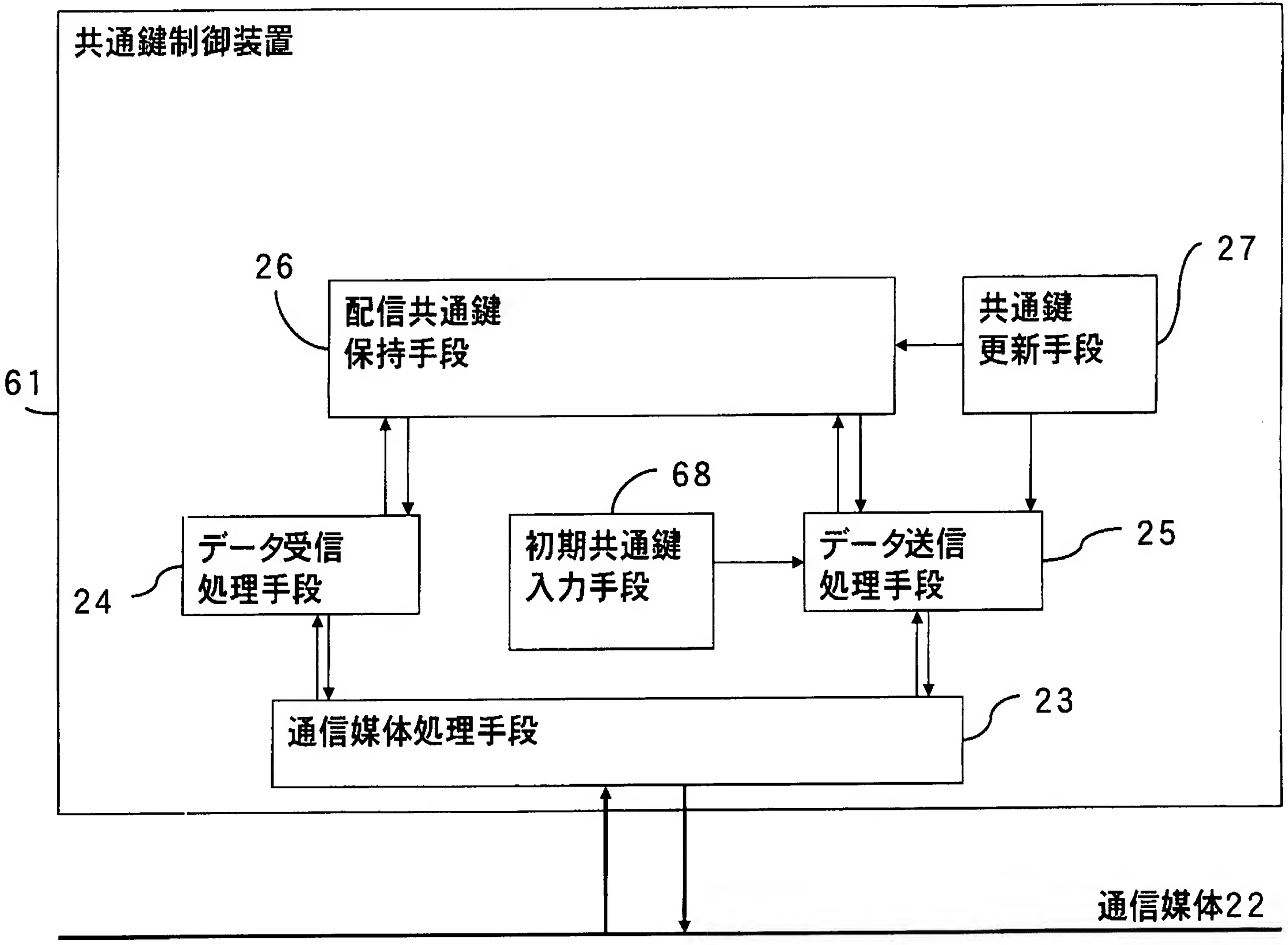

共通鍵制御装置
11
26
配信共通鍵
保持手段
共通鍵
更新手段
27
データ受信
処理手段
24
データ送信
処理手段
25
通信媒体処理手段
23
通信媒体22

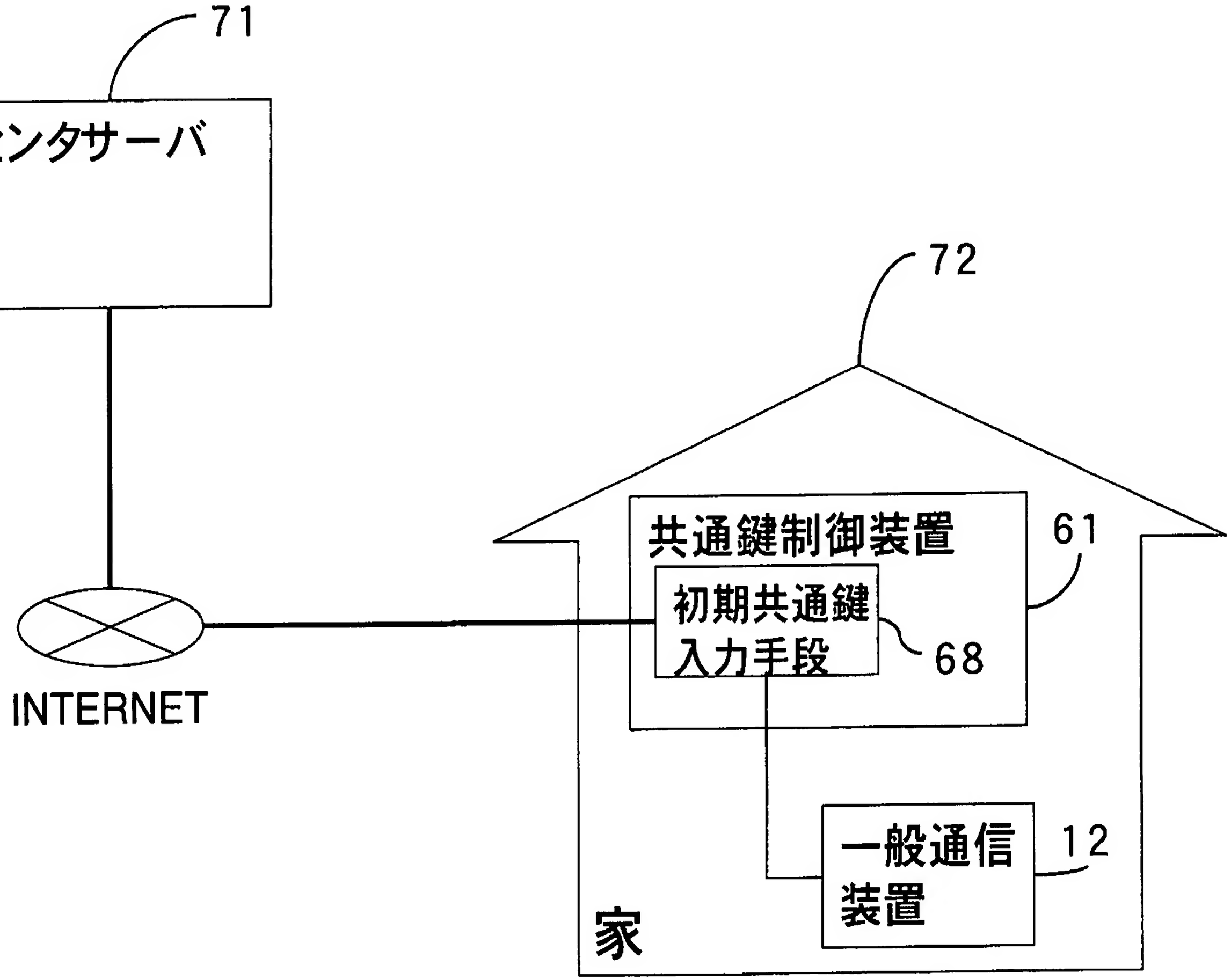

一般通信装置
12
36
共通鍵
保持手段
37
共通鍵
要求手段
34
データ受信
処理手段
35
データ送信
処理手段
33
通信媒体処理手段
通信媒体32

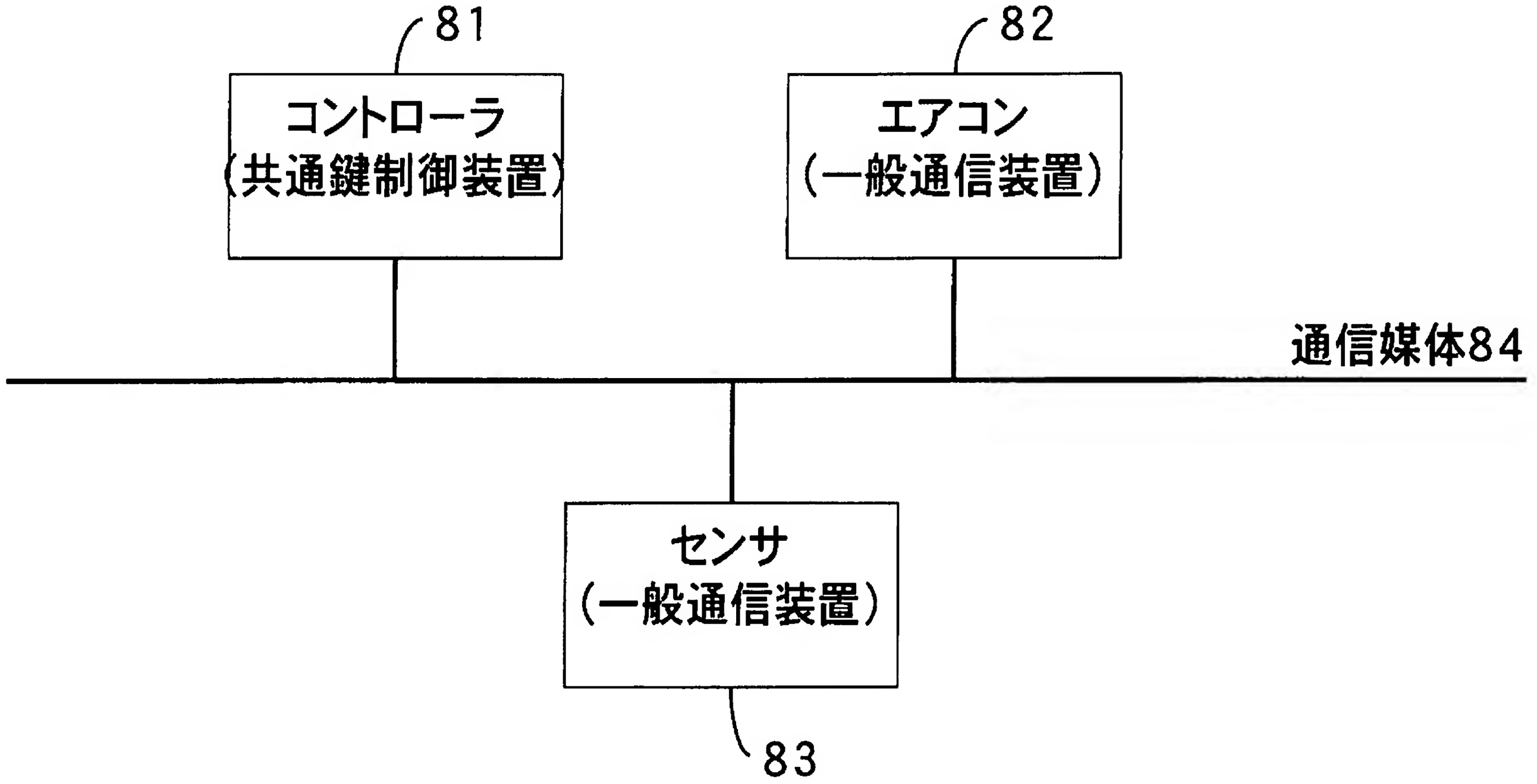

共通鍵
制御装置
一般
通信装置
一般通信装置の
共通鍵配信状態
一般通信装置の
送信時共通鍵
一般通信装置の
受信時共通鍵
共通鍵更新要求
更新完了
前共通鍵
前共通鍵
応答
配信完了
前共通鍵
前共通鍵
新共通鍵
共通鍵制御装置は、管理するすべての一般通信装置に共通鍵更新要求を送信
共通鍵移行設定要求
応答
移行中
新共通鍵
前共通鍵
新共通鍵
管理するすべての一般通信装置から新共通鍵設定応答受信時のみ共通鍵制御装置は、一般通信装置の共通鍵移行設定を更新完了にする。
共通鍵移行設定要求
応答
更新完了
新共通鍵
新共通鍵

51

共通鍵	配信先アドレス
最新共通鍵	アドレスA、アドレスB、アドレスC、・・・
共通鍵履歴1	アドレスD
共通鍵履歴2	アドレスE、アドレスF
共通鍵履歴4	アドレスG
・	・
共通鍵履歴 n	アドレスT


共通鍵制御装置
61
26
配信共通鍵
保持手段
27
共通鍵
更新手段
68
データ受信
処理手段
24
初期共通鍵
入力手段
データ送信
処理手段
25
通信媒体処理手段
23
通信媒体22


71
センタサーバ
INTERNET
72
共通鍵制御装置
61
初期共通鍵
入力手段
68
一般通信
装置
12
家


81
コントローラ
(共通鍵制御装置)
82
エアコン
(一般通信装置)
通信媒体84
センサ
(一般通信装置)
83

【書類名】 要約書

【要約】

【課題】共通鍵制御装置がネットワークに接続している一般通信装置が保持する共通鍵を更新する際、一般通信装置が複数存在する場合、更新前の共通鍵を保持する一般通信装置と、更新後の共通鍵を保持する一般通信装置がシステム内に混在し、一般通信装置間で通信ができない状況が発生する。

【解決手段】共通鍵を更新する中で、共通鍵配信状態を一般通信装置は保持する。一般通信装置が共通鍵を受信した際、自発的に共通鍵配信状態を変更することによって、また共通鍵制御装置が一般通信装置の共通鍵配信状態を設定することによって、一般通信装置がデータの送受信時に、更新前後のどちらの共通鍵を使用するかを決定する。その結果、更新前後の共通鍵が混在するシステムにおいても、一般通信装置間で通信を可能とする。

【選択図】図４

０００００５８２１
19900828
新規登録

大阪府門真市大字門真１００６番地
松下電器産業株式会社